BILLIN

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-0138]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, "Declared Public Health Emergency Exposure Records," DoD-0013. This system of records covers DoD's maintenance of records about individuals necessitated by a declared public health emergency (DPHE) by an appropriate official, including the Secretary of Health and Human Services pursuant to the Public Health Services Act, a DoD official, or other authorized state, local, or other governmental public health official pursuant to applicable law. These records are maintained to assist the DoD in establishing safe environments, identifying and protecting DoD-affiliated individuals at risk of transmission of or contracting the disease or agent at issue, and in supporting mission readiness. Additionally, the DoD is issuing a direct final rule, which is exempting this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn: Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Defense Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the Declared Public Health Emergency Exposure Records, DoD-0013 as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. The establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

DoD prioritizes the safety of its workforce to ensure Department's missions are able to be

accomplished successfully at all times in defense of the Nation. To do that, DoD must maintain operationally ready capabilities, including operating within degraded environments such as during a DPHE. Public health emergencies are varied; they may be broad or limited in geographical scope and may be declared by various authorities such as the Secretary of Health and Human Services or the responsible, designated State, local, tribal, or territorial official, or cognizant military commander. Responses to public health emergencies depend on the nature of the emergency, but in some cases the degraded environment created by the public health emergency may require the DoD to collect personal information to ensure a safe and secure workplace for employees and visitors to DoD facilities, and ultimately, to ensure DoD is able to continue to carry out its mission.

DoD Instruction 6200.03, "Public Health Emergency Management within the DoD," establishes DoD policy for DPHE. This includes the authority and responsibilities of DoD commanders and other officials during a DPHE, and various activities that may be required to address the emergency. For example, paragraph 3.1.d(1) provides that DoD may need to initiate actions to collect and analyze data on the health hazard causing the DPHE, and paragraph 3.1.d(3) provides that DoD may need to act to ensure identification, interview, and tracking of all individuals or groups suspected to have been exposed to the health hazard to characterize the source and spread of the health hazard. In carrying out these and other activities, DoD may collect and maintain information about individuals that is subject to the Privacy Act and therefore requires a SORN, but is not already covered by other DoD SORNs. Examples of the types of data in records that may be uniquely covered by this SORN include contact tracing data, which is the identification and contact information of individuals suspected or confirmed to have contracted a disease or illness, or exposed to an individual suspected or confirmed to have contracted a disease or illness, related to a DPHE; individual circumstances and dates of suspected exposure; and health status information. The data may also include information about individuals exposed to a public health threat other than a communicable disease such as a

radiological exposure or the release of a toxin or chemical agents, related to a DPHE. This system of records also supports the sharing of information that may need to occur during a DPHE, such as sharing of exposure information about individuals with public health authorities to support public health goals, such as contact tracing and the reduction of the spread of a health hazard.

The information covered by this system of records is separate and unique from other DoD systems of records which contain records maintained by DoD for accountability and assessment of DoD-affiliated personnel, or created during the normal course of DoD's delivery of occupational health and safety services, which DoD provides routinely to members of the military and DoD civilians, and sometimes to DoD visitors, concessionaires, and contractors. These records are covered by other SORNs, and are specifically identified in the notice below for clarity.

DoD maintains this information to ensure mission success through the appropriate management and response to the public health emergency, and to reduce the risk of disease or illness among DoD military and civilian personnel, contractors, concessionaires, and visitors to DoD facilities. The collection and use of records covered by this system of records is only permitted during times of a declared public health emergency.

Finally, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules, as amended by the Omnibus Final Rule, include the HIPAA Privacy Rule, the HIPAA Breach Rule, the HIPAA Security Rule, and the HIPAA Enforcement (Parts 160 and 164 of Title 45 CFR), permit a DoD covered entity to use or disclose protected health information for public health activities as noted in DoD Manual 6025.18. Under HIPAA, "public health authority" means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for

public health matters as part of its official mandate. 45 CFR 164.501 (definition of "public health authority"). The HIPAA Rules only apply if the entity or individual that is disclosing protected health information meets the definition of a HIPAA covered entity or business associate. The records covered under this SORN are not subject to the HIPAA Rules.

Additionally, the DoD is issuing a direct final rule to exempt this system of records from certain provisions of the Privacy Act elsewhere in today's issue of the *Federal Register*. DoD SORNs have been published in the *Federal Register* and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy, Civil Liberties, and Freedom of Information Directorate website at https://dpcld.defense.gov.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: December 9, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Declared Public Health Emergency Exposure Records, DoD-0013.

SECURITY CLASSIFICATION: Unclassified and classified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGERS: The system managers for this system of records are as follows:

A. Office of the Assistant Secretary of Defense for Health Affairs, Under Secretary of Defense (Personnel and Readiness), 1000 Defense Pentagon, Washington, DC 20301-1100.

B. Deputy Assistant Secretary of the Army, Office of the Surgeon General, U.S. Army Medical Command, 2050 Worth Road, Suite 13, Fort Sam Houston, TX 78234-6013.

C. Air Force Occupational Safety and Health (AFOSH), Department of the Air Force, 1000 Defense Pentagon, Washington DC 20301-1100, usaf.pentagon.af-a1.mbx.a1q--workflow@mail.mil.

D. Chief of Naval Personnel, Occupational and Environmental Medicine, Navy & Marine Corps Public Health Center, 620 John Paul Jones Circle, Suite 1100, Portsmouth, VA 23708-2103.

E. The Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records have been delegated to the DoD components. DoD components include the Military Departments of the Army, Air Force (including the U.S. Space Force), and Navy (including the U.S. Marine Corps), field operating agencies, major commands, field commands, installations, and activities. To contact the system managers at the DoD component with oversight of the records, go to www.FOIA.gov to locate the contact information for each component's Freedom of Information Act (FOIA) office.

AUTHORITY FOR MAINTAINANCE OF THIS SYSTEM: 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 2672, Protection of Buildings, Grounds, Property, and Persons and Implementation of Section 2672 of Title 10, United States Code; E.O. 14043, Requiring Coronavirus Disease 2019 Vaccination for Federal Employees; DoD Directive 5525.21, Protection of Buildings, Grounds, Property, and Persons; DoDI 6200.03, Public Health Emergency Management within the DoD; and DoDI 6055.17, DoD Emergency Management Program; or successor DoD policies, and E.O. 9397, as amended.

Note 1: The records covered under this SORN, while covered by the Privacy Act, are not subject to the HIPAA Rules.

PURPOSE(S) OF THE SYSTEM:

A. To support required or authorized activities during a declared public health emergency, such as contact tracing and coordination with medical and public health officials, for the purpose of maintaining safe and healthy DoD environments, including work and training environments, transportation facilities and vehicles, base housing, retail and recreation areas, hospitals, and other health care facilities.

B. To support the managing, monitoring, tracking, reporting and sharing of records created during a declared public health emergency to protect DoD Service members and their dependents, the civilian workforce, contractors, concessionaires, and visitors to DoD facilities.

C. To identify and protect individuals at risk for transmitting or contracting a communicable disease related to a declared public health emergency; to identify and protect those who may be at elevated risk of symptomatic or severe disease from a public health threat, such as a communicable disease or biohazard, or exposure to radiation, toxins, or chemical agents; and to limit exposure to the source(s) of infection or illness through public health mitigation and surveillance activities, such as monitoring and contact tracing.

D. To support DoD and non-DoD health care personnel, including public health officials, who need to collect, use, and review this information in performance of their duties related to the public health emergency or to delivering health care to affected individuals.

E. To support use of this information by other DoD officials to determine mission readiness and conduct after-action reviews. Statistical data instead of identifiable information will be used wherever practicable for these efforts.

Note 2: A declared public health emergency may be limited or broad in geographic scope, and could affect one, many, or all DoD installations and facilities. This system of records may support worldwide DoD public health emergency activities in the case of a pandemic, or local or regional DoD activities in the case of a geographically limited public health emergency.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: DoD military Service members (Active Duty, Guard/Reserve, and Coast Guard personnel when acting as a military service with the Navy), civilian personnel (including non-appropriated fund employees), DoD spouses/dependents and cohabitants, military retirees, and DoD contractors. Also, personnel of partner organizations, visitors, eligible patrons, or concessionaires accessing or sharing DoD facilities or attending DoD-sponsored events, and individuals residing in military housing during a declared public health emergency, including a pandemic.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Personal and Employment Information: name, Employee Identification Number / DoD ID number, Social Security Number, date of birth, gender, address, phone number(s), email(s), demographic or biographical information, recent domestic and international travel and status (e.g., Service member, dependent, civilian, contractor, visitor, etc.); emergency contact information (emergency contact's name, phone number, address, email address, and relationship to the individual); employment information (title, organizational affiliation, duty location); employment time and attendance records; disability information; personnel accountability information (such as current work status of the individual and affiliated leave status information).

B. Medical Information: confirmed medical test results, physician assessment of medical transmission risk status (either for the individual or because the individual cohabitates with others who may be considered medically high-risk); medical diagnoses and prognosis information; dates of medical visits or tests, individual symptoms; potential or actual exposure to the public health threat (e.g., biohazard or communicable disease); medical history related to the treatment of a virus or communicable disease essential to mitigate the spread of disease during a public health emergency; immunizations and vaccination information; medical directives and/or expressions of interest in receiving a vaccine or other medical treatments, religious or other objections to medical treatment; correspondence with individuals or medical/family representatives on medical treatment; medical, treatment, or disclosure consent forms;, medical or health emergency notification forms.

C. Contact Tracing Information: proximity tracking information of individuals after diagnosis or suspected exposure, to include dates when the individual visited a DoD facility or attended a DoD-sponsored event, the locations visited within the facility (e.g., floor, room number), time duration spent in the facility, and identification of persons in contact with while at the facility; records that indicate an individual's location and/or proximity to others on DoD property or at the event over time as compiled through either manual or through technical means (such as badge access, office location, and information technology system login information; and any other relevant information completed, obtained, or developed as a result of an individual attending, working or entering a DoD facility/event during a public health emergency).

Note 3: Excluded from this system of records are employee occupational medical records covered by the U.S. Office of Personnel Management (OPM) regulation at 5 CFR part 293, subpart E, Employee Medical File System Records. The regulation requires agencies that are subject to OPM's recordkeeping requirements to maintain employee occupational medical records in the agency's Employee Medical File System. Such records are covered exclusively by the OPM/GOVT-10, Employee Medical File System of Records.

Note 4: Excluded from this system of records are DoD accountability and assessment records as described in DoD-0012, Defense Accountability and Assessment Records SORN. Records in DoD-0012 are collected and used to account for DoD-affiliated personnel in a natural or man-made disaster, during a public health emergency, or when directed by the Secretary of Defense. During a declared public health emergency, DoD may collect and maintain records under both the DoD-0012 SORN to support DoD accountability and assessment for DoD-affiliated individuals, and this SORN to support contract tracing and other authorized public health objectives necessitated by the declared public health emergency.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Individuals, healthcare personnel, entities designated as public health authorities, and information systems maintaining data described in the Categories of Records section above, such as DoD medical systems, DoD human resources/personnel systems, DoD identity and credentialing software for information technology systems; and visitor, security, and access control systems for DoD facilities or locations where DoD-sponsored events are held. When the individual is a minor or is otherwise unable to provide information about themselves due to illness or other incapacity, DoD may collect information from appropriate sources such as family members, co-workers, friends, or co-habitants for the purposes described in this notice.

ROUTINE USES AND RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as Routine Use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1)

responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act of 1978, as amended.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statue or treaty.

K. To Federal, State, local, foreign, or international public health agencies and officials, including the Centers for Disease Control and Prevention, to the extent necessary to comply with laws or policies governing reporting on the impact of a communicable disease, agent, or other cause responsible for the declared public health emergency.

L. To an emergency contact for purposes of locating an individual to communicate possible exposure to or treatment options for a public health threat such as a communicable disease or exposure to a biohazard.

M. To the U.S. Department of State when it requires information to consider or provide an informed response to a request for information from a foreign, international, or intergovernmental agency, authority, or organization about public health relating to DoD personnel, facilities, or activities abroad.

N. To individuals for the purpose of determining if they have had contact with a person known or suspected to have a communicable disease, illness, or other exposure that requires quarantine, and to identify and protect the health and safety of others who may have been exposed.

O. To hospitals, physicians, and other healthcare providers for the purpose of protecting the health and safety of individuals who may have been exposed to a contagion or biohazard, or to assist such persons or organizations in preventing exposure to or transmission of a communicable disease.

P. To Federal, state, local, tribal, territorial, or foreign governmental agencies; multilateral governmental organizations; medical facilities or providers, or other public health entities, for the purpose of protecting the vital interests of a record subject or other persons, including to assist such agencies or organizations during an epidemiological investigation, in facilitating continuity of care, or in preventing exposure to or transmission of a communicable disease or biohazard of public health significance.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by an individual's name and/or individual identification number, such as Social Security Number or DoD ID Number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are to be retained by the Office of the Secretary of Defense, the Joint Staff, the Military Departments, the Defense Agencies, and the Defense Field Activities in accordance with their NARA-approved records retention schedules.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable

information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

Personal information maintained will be the minimum necessary and only used for the purposes stated in this notice. Such information will be retained for the minimum amount of time, remain accessible only to personnel with a valid operational need, and only be used for the public health emergency and no other purposes. These records may be provided in aggregate for accountability and mission readiness purposes, as long as the information may not be easily re-identified.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the

individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3); (d)(1), (2), (3), and (4); (e)(1); (e)(4)(G), (H), and (I); and (f) pursuant to 5 U.S.C. 552a(k)(1). In addition, when exempt records received from other systems of records become part of this system, the DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records of which they were a part, and claims any additional exemptions set forth here. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e), and published in 32 CFR part 310.

HISTORY: None.

[FR Doc. 2022-27150 Filed: 12/15/2022 8:45 am; Publication Date: 12/16/2022]